SANDIA REPORT

SAND2006-5560
Unlimited Release
Printed August 2006

Final LDRD Report
Human Interaction with Complex Systems:
Advances in Hybrid Reachability and Control

Meeko M.K. Oishi

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94-AL85000.

Sandia National Laboratories

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online ordering: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2006-5560
Unlimited Release
Printed August 2006

Final LDRD Report
Human Interaction with Complex Systems: Advances in Hybrid Reachability and Control

Meeko Oishi
Truman Postdoctoral Fellow
Sandia National Laboratories
P.O. Box 5800
Albuquerque, NM 87185-1137
mmoishi@sandia.gov

Abstract

This document describes new advances in hybrid reachability techniques accomplished during the course of a one-year Truman Postdoctoral Fellowship. These techniques provide guarantees of safety in complex systems, which is especially important in high-risk, expensive, or safety-critical systems. My work focused on new approaches to two specific problems motivated by real-world issues in complex systems: 1) multi-objecitve controller synthesis, and 2) control for recovery from error. Regarding the first problem, a novel application of reachability analysis allowed controller synthesis in a single step to achieve a) safety, b) stability, and c) prevent input saturation. By extending the state to include the input parameters, constraints for stability, saturation, and envelope protection are incorporated into a single reachability analysis. Regarding the second problem, a new approach to the problem of recovery provides a) states from which recovery is possible, and b) controllers to guide the system during a recovery maneuver from an error state to a safe state in minimal time. Results are computed in both problems on nonlinear models of single longitudinal aircraft dynamics and two-aircraft lateral collision avoidance dynamics.

Contents

List of Figures

1 Introduction

Human-automation systems are automated systems with which a human interacts. These types of systems are ubiquitous, occurring in scientific research platforms (unmanned ocean-, and aerial-vehicles), military systems (fleets of ground vehicles, micro-scale platforms), critical infrastructures (the power grid, the US water supply), transportation systems (automobiles, commercial aircraft, air traffic control), and consumer products (alarm clocks, VCRs, cellular phones), for example. In many of these systems, the automation controls low-level functions while the human provides supervisory or high-level commands. In high-risk, expensive, or safety-critical applications, the way in which a human interacts with the automation is paramount to the correct and safe operation of the system. As computing power continues to grow and embedded automation becomes commonplace, the range of applications for human-automation systems will only increase. However, despite the widespread use and growing presence of human-automation systems, there is a clear need for advances in tools and methods to analyze and control the performance of human-automation systems. This is especially true for human-automation systems which are large, complex, or highly interconnected [1, 2, 3, 4]. Consider, for example, commercial aircraft, in which problems in human interaction with the automation can have serious (or even fatal) consequences [5].

One approach to this problem is through the use of formal methods, which can provide mathematical guarantees that a complex system satisfies a certain property of its state-space. Formal methods are complementary to efforts in human factors research and in large-scale simulation. For complex systems with changing dynamics (*hybrid systems*), control theorists and computer scientists have developed formal methods in *reachability analysis* to prove the safety of complex systems. New methods and tools in reachability analysis can provide an alternative framework for control design in safety-critical systems such as civil jet aircraft. These methods provide a mathematical guarantee of the modeled system's behavior, in the presence of state and input constraints.

Reachability problems are often posed in terms of maintaining a certain property of the state-space. This is a non-trivial problem when the control input for such a system is bounded. For these types of systems, information is often given about "good" or "bad" regions of the state-space: the system should avoid certain "bad" regions or remain within certain "good" regions. For example, during flight, an aircraft must remain within its aerodynamic flight envelope, a "good" region of the aircraft's state-space. Flight envelopes are often defined in terms of the aircraft's speed, flight path angle, and altitude. Leaving the flight envelope could result in a stall, structural damage, or, in the case of civil jet aircraft, significant passenger discomfort. We can mathematically guarantee that the aircraft will never leave its flight envelope using results from a continuous reachability analysis and controller synthesis.

While algorithms and computational methods have been concertedly developed over the past decade for fully-automated systems, less is known about how these methods must change in order to accommodate human interaction with automated systems. My research aims to extend known reachability tools to directly account for the human and to provide guarantees of behavior that can be implemented on actual systems. Over the past year as a Truman Postdoctoral Fellow I have focused on two specific problems in reachability analysis for human-automation systems: 1) multi-objective controller synthesis, and 2) recovery from error. Both of these problems are addressed through new applications and extensions of hybrid reachability analysis and controller synthesis.

An aircraft incident Paris-Orly, France highlights issues regarding both multi-objective controller synthesis, as well as guided recovery from error. During the aircraft's final approach to landing, the pilot inadvertently and unknowingly activated envelope protection control laws. Upon reaching a speed excessive for the aircraft's aerodynamic configuration, the autopilot initiated an altitude-change maneuver, in order to avoid

structural damage to the wing. This initially caused the aircraft to climb steeply. The autothrottles increased the thrust, while the pilots attempted to use the aircraft's control surfaces to make the aircraft descend. However, the envelope protection control laws overrode the pilot's actions, commanding a high angle of attack, and eventually reaching a stall. The flight crew managed to regain control of the aircraft, then successfully completed a manual landing [6, 5].

Multi-objective controller synthesis involves the problem of control design for multiple goals, including safety, stability, and input non-saturation. In complex systems such as aircraft, many of these control goals must be achieved simultaneously. Blindly implementing control schemes for multiple goals (e.g. envelope protection and stabilization) can result in chattering, instability, and other counterintuitive phenomenon, when the controller switches between multiple, independently designed control laws. My approach avoids these problems through the synthesis of a single controller to fulfill all three goals simultaneously. This controller is computed through a carefully formulated reachability problem.

Recovery from error is a practical problem that arises in designing to accommodate potential failures. This is paramount for safe operation of complex systems such as civil jet aircraft [7]. These systems require not only design and operational procedures to prevent failures in the first place, but also additional control guidance and procedures for recovery in the event that a failure does occur. Many potential failures are discovered through extensive simulation in order to help identify and address unanticipated problems, however it is physically impossible to test all possible initial conditions. Problems which go undetected through this design and simulation process can result in "automation surprises" [8] and other problematic behaviors in actual aircraft operation. My approach is two-fold: 1) a standard reachability analysis to determine the minimum requirements for safety, and 2) a modified reachability analysis to determine how, in the event of deviation from the computed safe regions, recovery can be achieved. Under these circumstances, recovery is only possible when some flexibility can be exploited in the system (e.g. temporarily relaxed constraints, additional control authority).

This report first provides a basic introduction to established results in reachability analysis and controller synthesis. The remainder of the report focuses on novel contributions to reachability analysis that were accomplished this past year. Each section details the mathematical problem formulation, solution method, and application to real-world examples. The main contributions are summarized in the conclusion.

2 Background: Hybrid Reachability

We define safety as the ability to remain within a set of constraints in the continuous state-space, despite bounded control authority. We can compute, through standard reachability analysis and controller synthesis, the subset of those states in which we can guarantee the state of the system can always remain: this is the *invariant set*, which determines the "safe" region of operation [9]. States outside of this set comprise the *reachable set*, those states which can "reach" constraint violation. This technique, computationally based on a Hamilton-Jacobi partial differential equation (HJ PDE), also synthesizes a set-valued control law which enforces safety by preventing the state of the system from entering the reachable set. We draw on the Hamilton-Jacobi techniques here because of their sub-grid accuracy and success in previous aircraft applications [10, 11, 12], however viability techniques could also be used. Viability theory [13] and numerical algorithms [14] have been developed to compute viability kernels and capture basins for continuous systems, and also extended to hybrid systems [15, 16]. These are computationally based on a minimum-time-to-reach formulation [17].

Through reachability analysis and controller synthesis we can determine the *invariant set* $\mathscr{W} \subseteq \mathscr{C} \subseteq \mathbb{R}^n$, consisting of those initial states for which there exists at least one trajectory that will not exit the constraint set $\mathscr{C}$. We denote the complement of the invariant set, also known as the reachable set, as $\overline{\mathscr{W}}$. Given a dynamically evolving system (21) and a constraint set $\mathscr{C}$, we define the *backwards reachable set* $\overline{\mathscr{W}(t)}$ as the set of all states which will exit the constraint set $\mathscr{C}$ in the time $[0,t]$. To calculate the invariant set, define a continuous function $J_0 : \mathscr{X} \to \mathbb{R}$ such that

$$\mathscr{C} = \{x \in \mathscr{X} \,|\, J_0(x) \geq 0\}. \tag{1}$$

The backwards reachable set $\overline{\mathscr{W}(t)}$ can be found by solving the terminal value Hamilton-Jacobi (HJ) partial differential equation (PDE) [18, 9, 11]

$$\begin{aligned} \frac{\partial J(x,t)}{\partial t} + \min\left[0, H\left(x, \frac{\partial J(x,t)}{\partial x}\right)\right] = 0 \qquad & \text{for } t < 0; \\ J(x,0) = J_0(x) \text{ for } t = 0; & \end{aligned} \tag{2}$$

As shown in [11], we obtain an implicit representation of the invariant set $\mathscr{W}(t) = \{x \in \mathscr{X} | J(x,-t) \geq 0\}$. If (2) converges as $t \to -\infty$, $J(x,-t) \to J(x)$, and the reachable set converges to a fixed point $\overline{\mathscr{W}(t)} \to \overline{\mathscr{W}}$. The invariant set is defined as $\mathscr{W}$, the complement of the reachable set.

The state-dependent control

$$u^*(x) = \{u \in \mathscr{U} \mid \left(\frac{\partial J(x)}{\partial x}\right)^T f(x,u) \geq 0\}. \tag{3}$$

synthesized from the above calculation must be applied along the boundary of the invariant set in order to prevent trajectories which reach the boundary of the invariant set from exiting.

The *forward reachable set* computation proceeds similarly in forwards time, with an additional constraint due to the avoid set $\mathscr{A}$, defined by the continuous function $J_A : \mathscr{X} \to \mathbb{R}$ such that $\mathscr{A} = \{x \in \mathscr{X} \,|\, J_A(x) \geq 0\}$. We define the function $J_A(x)$ as positive for states inside the avoid set $\mathscr{A}$. The cost function evolution is constrained by

$$J(x,t) \leq J_A(x) \text{ for } t \geq 0 \tag{4}$$

so that the reachable set cannot enter the avoid set $\mathscr{A}$. Further details can be found in [18, 12].

3 Multi-Objective Controller Synthesis

The main contribution presented here is a one-step technique to find non-saturating feedback linearizing controllers through application of reachability techniques which guarantee envelope protection. As opposed to a multi-step process, in which control laws for different goals are synthesized independently, our method assures simultaneous fulfillment of multiple control goals: stabilization, envelope protection, and input non-saturation. While a standard reachability analysis could guarantee that envelope protection and input non-saturation could be simultaneously met, the resultant control law would not guarantee stability and would not necessarily be implementable – it could likely be bang-bang or cause chattering. Therefore, our approach uses a reachability calculation with additional constraints to ensure that the resultant control law meets all the desired objectives and is implementable, as well.

To address the problem of envelope protection, we define safety as the ability to remain within a set of constraints in the continuous state-space, despite bounded control authority. We can compute, through standard reachability analysis and controller synthesis, the subset of those states in which we can guarantee the state of the system can always remain: this is the *invariant set*, which determines the "safe" region of operation [9]. States outside of this set comprise the *reachable set*, those states which can "reach" constraint violation.

To address stabilization under saturation, we parameterize feedback linearizing control laws subject to bounded control input, such that the parameters reflect system performance goals (i.e. damping, overshoot, etc). We formulate constraints that input saturation and stability place on the input parameters. Feedback linearization is a popular technique for differentially flat systems [19, 20], but can generate inputs with high-magnitude. Synthesizing non-saturating feedback linearizing control laws is a non-trivial problem [21, 22, 23] for stabilization [24] as well as for tracking [25]. Work in trajectory generation for differentially flat systems has addressed systems subject to saturation and rate constraints [26, 27]. Other common techniques to incorporate state and input constraints have made use of model predictive control [28, 29, 30], and of control Lyapunov functions [31, 32], however finding such functions is often difficult and done heuristically. For linear systems, quadratic Lyapunov functions can be synthesized [33, 34].

3.1 Problem Formulation

Consider the input-output full-state feedback linearizable system

$$\begin{array}{rcl} \dot{x} & = & f(x)+g(x)u, x \in \mathscr{X} \subseteq \mathbb{R}^n, u \in \mathbb{R} \\ y & = & h(x), y \in \mathbb{R} \end{array} \tag{5}$$

with bounded input $u \in \mathscr{U}$, and constraint set $\mathscr{C} \subset \mathbb{R}^n$ which encodes the set of states which satisfy the constraints on the system (e.g., speeds above the aircraft's stall speed). We express the state constraints through the inequality

$$\mathscr{C} = \{x \,|\, c(x) \geq 0\}. \tag{6}$$

The feedback linearizing control law to stabilize (5) around the equilibrium $x^* = 0$ is

$$u(x,\beta) = \frac{1}{L_g h}\left(-L_f^{(n-1)}h - \sum_{i=0}^{n-1}\beta_i x^{(i)}\right) \tag{7}$$

with Lie derivatives $L_f h = \frac{\partial h}{\partial x} f(x)$, $L_f^2 h = \frac{\partial^2 h}{\partial x^2} f(x)$, $\cdots$, $L_f^{(n-1)} h = \frac{\partial^{(n-1)} h}{\partial x^{(n-1)}} f(x)$, and $x^{(i)}$ the ith time derivative of x. Constant coefficients $\beta = [\beta_0, \beta_1, \cdots, \beta_{n-1}]$ are chosen such that the polynomial $\sum_{i=0}^{n-1} \beta_i X^i(s)$ is

Hurwitz. With this control law, the resultant closed-loop system will be linear and stable. However, in order to prevent saturation, the control $u(x,\beta)$ must remain within its allowable bounds $\mathscr{U}$ for a constant β for $x \in \mathscr{X}$.

$$u_{\min} \leq u(x,\beta) \leq u_{\max} \tag{8}$$

We wish to satisfy two goals with a single controller: 1) envelope protection, and 2) stabilization under saturation. Further, we wish to determine the largest set of states from which this controller is guaranteed to fulfill these goals.

Statement of Problem 1 *Given the dynamical system (5), with state constraints (6), and with a feedback linearizing control law $u(x,\beta)$ (7) parameterized by a constant vector $\beta \in \mathbb{R}^n$, determine 1) the invariant set $\mathscr{W}$, which is the largest set of states x for a given non-saturating controller $u(x,\beta)$ that will reach the origin without violating the state constraints $x \in \mathscr{C}$, 2) β such that the feedback linearizing control law is both non-saturating (8) and stable.*

3.2 Method

We first append the parameter vector β to the state such that $\tilde{x} = [x,\beta] \in \mathbb{R}^{2n}$, with zero dynamics to ensure that β remains a constant in the reachability computation. We then incorporate state, stability, and input constraints into the initial cost function and run a reachability calculation with this initial value. Note that for first and second-order systems, the requirements for stability simplify to $\beta_i > 0$.

Solution of Problem 1 *For the dynamical system with extended state $\tilde{x} = [x,\beta]$*

$$\begin{array}{rcl} \dot{x} & = & f(x) + g(x)\left(-L_f^{n-1}h - \frac{1}{L_g h}\sum_{i=0}^{n-1}\beta_i x^{(i)}\right) \\ \dot{\beta} & = & 0 \end{array} \tag{9}$$

define the initial cost function

$$J_0(x,\beta) = \min\left\{J_0^{\text{state}}(x,\beta), J_0^{\text{sat}-\max}(x,\beta), J_0^{\text{sat}-\min}(x,\beta), J_0^{\text{stability}}(x,\beta)\right\} \tag{10}$$

with $J_0^{\text{state}}(x,\beta) = c(x)$, $J_0^{\text{sat}-\max}(x,\beta) = u_{\max} - u(x,\beta)$, $J_0^{\text{sat}-\min}(x,\beta) = u(x,\beta) - u_{\min}$, $J_0^{\text{stability}}(x,\beta) = \beta_i$ such that they are positive in those regions where the constraints are satisfied. The result of a reachability computation run with initial cost function (10) is the invariant set $\mathscr{W}$, the largest set of x for which a given β will stabilize (9) without violating state (6) or input (8)constraints.

The advantage of this framework is that the computed result inherently meets the required constraints for both stability and non-saturation, while determining how to keep the state of the system within its constraint set. For a given β, the computed result provides the region of the state-space for which the specified controller will stabilize, will not saturate, and will not violate any of the state bounds. This technique is extendable to to input-output feedback linearizable systems which are minimum phase and to multiple input-multiple output systems.

While dimensionality is a critical issue in any reachability calculation, one potential pitfall of this method is that it requires augmenting the state-space by at most n dimensions. However, one remedy to this is to take advantage of structure in the pole placement of the closed-loop system. If, for example, poles are collocated on the real line, then $\beta_1 = \eta^2$ and $\beta_2 = 2\eta$. By parameterizing β the reachability calculation can be done in a total of $n+1$ dimensions in (x,η).

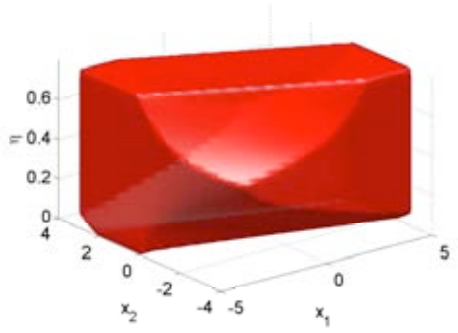

Figure 1: Invariant set $\mathscr{W}_\beta$ plotted in (x_1, x_2, η) for $\eta = 0.35$, corresponding to two real poles at -0.5766 and -0.1734.]

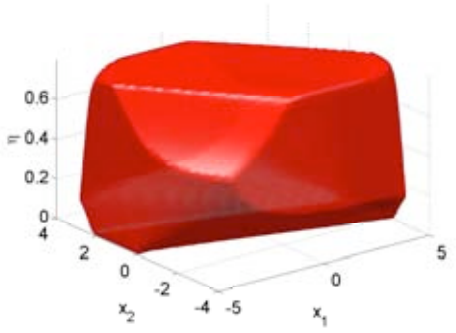

Figure 2: Invariant set $\mathscr{W}_\beta$ plotted in (x_1, x_2, η) for $\eta = 0.30$, corresponding to an imaginary pair at $-0.15 \pm 0.5268i$.

3.3 Examples

Double Integrator

To demonstrate this method, consider the system $\ddot{x} = u$, with state $x = [x_1, x_2] \in \mathscr{C} = \mathscr{X} = [\underline{x}_1, \bar{x}_1] \times [\underline{x}_2, \bar{x}_2]$, input $u \in \mathscr{U} = [u_{\min}, u_{\max}]$, and output $h = x_2$. We design a feedback linearizing control law, $u(x, \beta) = -\beta_1 x_1 - \beta_2 x_2$, with $\beta_1, \beta_2 \in \mathbb{R}^+$, such that the resultant closed-loop system is stable.

We consider two cases: 1) two real poles when $\beta_1 = \eta^2$, $\beta_2 = \eta$, and 2) two imaginary poles when $\beta_1 = \beta_2 = \eta$. The constraint set $\mathscr{C} \subseteq \mathscr{X} \times \mathbb{R}^+$ incorporates both the state constraint $x \in \mathscr{C}$ as well as the input constraint $u(x, \beta) \in \mathscr{U}$. The saturation constraints (8), state constraints, and stability constraints are formulated as

$$\begin{aligned} J_0^{\text{sat}}(x, \beta) &= \min\{u_{\max} - \beta_1 x_1 - \beta_2 x_2, -\beta_1 x_1 - \beta_2 x_2 - u_{\min}\} \\ J_0^{\text{state}}(x) &= \min\{\bar{x}_1 - x_1, x_1 - \underline{x}_1, \bar{x}_2 - x_2, x_2 - \underline{x}_2\} \\ J_0^{\text{stability}}(\beta) &= \eta. \end{aligned} \tag{11}$$

For the reachability computation, we combine the above three functions into one initial cost function

$$J_0(x, \beta) = \min\{J_0^{\text{sat}}(x, \beta), J_0^{\text{state}}(x), J_0^{\text{stability}}(\beta)\} \tag{12}$$

Each horizontal slice in Figures 1 and 2 represents the invariant set in $[x_1, x_2]$ for a given input parameter η. It is the set of initial conditions for which the state will be driven to the equilibrium without saturating the input or violating the state constraints. Figures 3 and 4 show the largest invariant sets for given β vectors.

Aerodynamic Envelope Protection

We model the longitudinal dynamics of a conventional aircraft as a nonlinear system

$$\begin{aligned} m\dot{V} &= T - D(\alpha, V) - mg \sin\gamma \\ mV\dot{\gamma} &= L(\alpha, V) - mg \cos\gamma \end{aligned} \tag{13}$$

with state $x = [V, \gamma] \in \mathscr{X} = \mathbb{R}^+ \times \mathbb{R}$ (corresponding to speed V and flight path angle γ) input $u = [T, \alpha] \in \mathscr{U} = [T_{\min}, T_{\max}] \times [\alpha_{\min}, \alpha_{\max}]$ (corresponding to thrust T and angle of attack α). The state constraints are

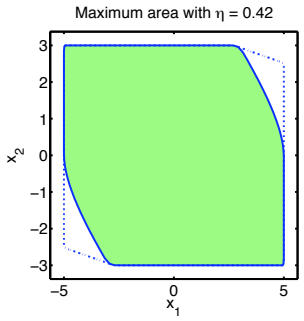

Figure 3: Largest invariant set with two real poles, plotted in (x_1, x_2) for $\eta = 0.42$.

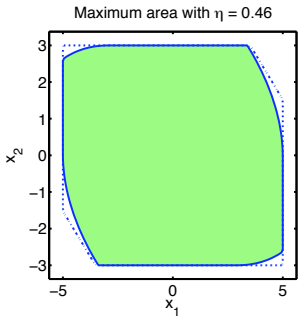

Figure 4: Largest invariant set with an imaginary pair of poles, plotted in (x_1, x_2) for $\eta = 0.46$.

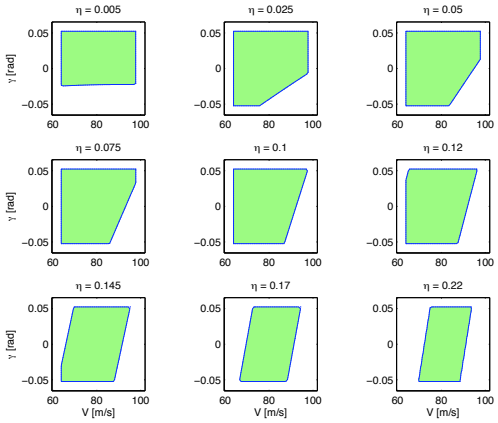

Figure 5: Horizontal slices of Figure 6 show the invariant set in (V, γ) at various η which correspond to stabilizing and non-saturating control laws.

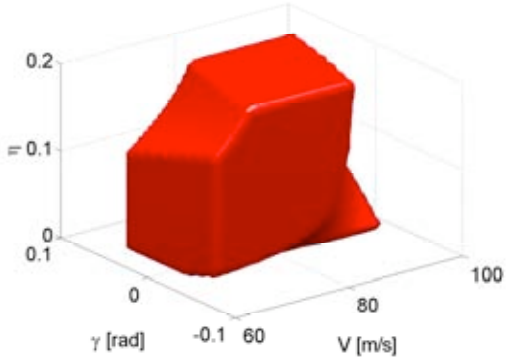

Figure 6: Invariant set in (V, γ, η). For a given η, states inside the shaded region will reach (V_r, γ_r) without saturating the input or violating the aerodynamic envelope.

given by $x \in \mathscr{C} = [V_{\min}, V_{\max}] \times [\gamma_{\min}, \gamma_{\max}] \subseteq \mathscr{X}$. Physical constants are mass $m = 200000$ kg, gravitational constant $g = 9.81 \text{m/s}^2$, and the sets $\mathscr{X} = [63.79, 97.74] \times [-6, 6]$, $\mathscr{U} = [0, 686700] \times [-5, 17]$ are determined by standard aircraft operating conditions. Drag and lift are given by

$$\begin{array}{rcl} D(\alpha, V) & = & V^2(a + bc_L(\alpha)^2) \\ L(\alpha, V) & = & cV^2 c_L(\alpha) \end{array} \tag{14}$$

with coefficient of lift $c_L(\alpha) = c_{L_0} + c_{L_\alpha}\alpha$, and positive constants $a = 6.5106$, $b = 12.6585$, $c = 262.0275$, $c_{L_0} = 0.4225$, and $c_{L_\alpha} = 5.105$ as in the Flaps-20 configuration of the large civil jet aircraft with its landing gear up [10]. The aircraft should track a reference speed $V_r = 90$ m/s and a reference flight path angle $\gamma_r = 0^\circ$.

By choosing the control law

$$u(x, \beta) = \phi^{-1}\left(\begin{bmatrix} mg\sin\gamma + aV^2 - m\beta_1(V - V_r) \\ \frac{1}{cV^2}(mg\cos\gamma - mV\beta_2(\gamma - \gamma_r)) \end{bmatrix} \right), \; \overline{u} \triangleq \phi(u) = \begin{bmatrix} -bV^2 c_L(\alpha)^2 + T \\ c_L(\alpha) \end{bmatrix} \tag{15}$$

with $\beta_1, \beta_2 \in \mathbb{R}^+$, (13) will track $x_r = [V_r, \gamma_r]$.

We assume that $\beta_1 = \beta_2 = \eta$, and incorporate the state, input, and stability constraints into the initial cost

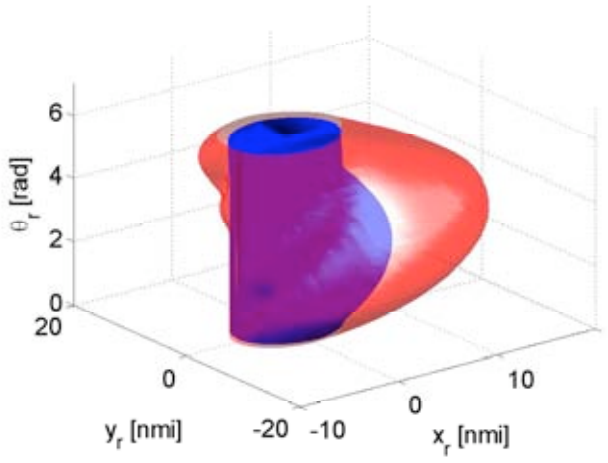

Figure 7: States outside the transparent (red) solid represent the invariant set in (x_r, y_r, θ_r) for feedback linearizing control with $\beta = 1.10 \times 10^{-3}$. States outside the opaque solid (blue) represent the invariant set with optimal control.

function:

$$J_0(x,\beta) = \min\{J_0^{\text{sat}}(x,\beta), J_0^{\text{env}}(x), \beta\} \tag{16}$$

with $J_0^{\text{sat}}(x,\beta) = \min\{u_{\max} - u(x,\beta), u(x,\beta) - u_{\min}\}$, $J_0^{\text{state}}(x,\beta) = \min\{V_{\max} - V, V - V_{\min}, \gamma_{\max} - \gamma, \gamma - \gamma_{\min}\}$.

The result of the reachability calculation is shown in Figure 6 for combinations of $[V, \gamma, \eta]$. For clarity, cross-sections of $[V, \gamma]$ for various η are shown in Figure 5. As the control parameter increases, less of the aerodynamic flight envelope (V, γ) is controllable, due mainly to input saturation. The uncontrollable portions of the (V, γ) envelope at all η in the lower right quadrant correspond to descent at high speeds – this is a well-known issue for landing aircraft, in which the aircraft is very close to a stall condition. The maximum area controllable set occurs at $\eta = 0.045$, which will allow for operation in more combinations of speed and flight path angle than any other envelope in the computed set $\mathscr{W}$.

Cooperative Collision Avoidance

We model the relative dynamics of two aircraft traveling at a constant speed $V = 0.125$ nmi/s,

$$\begin{bmatrix} \dot{x}_r \\ \dot{y}_r \\ \dot{\theta}_r \end{bmatrix} = V \begin{bmatrix} \cos(\theta_r - \theta_R) - 1 \\ \sin(\theta_r - \theta_R) \\ 0 \end{bmatrix} - \frac{V}{g} \begin{bmatrix} y_r & 0 \\ -x_r & 0 \\ -1 & 1 \end{bmatrix} u \tag{17}$$

with relative position x_r, y_r, relative heading θ_r, turn rates $u_1, u_2 \in [-\tan(2\pi/9), \tan(2\pi/9)]$, and constant $g = 5.3 \times 10^{-3}$ nmi/s^2. As opposed to the competitive model presented in [35], we assume cooperative, centralized control over both aircraft. For ease of notation, we write (17) as $\dot{x} = F(x) + G(x)u$, where $F(x) \in \mathbb{R}^3$ and $G(x) \in \mathbb{R}^{3\times 2}$. The aircraft must remain at least $R = 5$ nmi apart at all times, so the state is constrained by

$$J_0^{\text{radius}}(x) = x_r^2 + y_r^2 - R^2 \geq 0 \tag{18}$$

Assuming cooperation between the two aircraft and full-state output $y = [x_r, y_r, \theta_r]$, the feedback linearizing control

$$u(x,\beta) = \left(G^T G\right)^{-1} G^T \left(\begin{bmatrix} \beta_1 x_r \\ \beta_2 y_r \\ \beta_3(\theta_r - \theta_R) \end{bmatrix} - F(x) \right) \tag{19}$$

tracks a desired relative heading θ_R, subject to saturation constraints $J_0^{\max}(x,\beta) = u_{\max} - u(x,\beta)$, $J_0^{\min}(x,\beta) = u(x,\beta) - u_{\max}$. We parameterize β by $\beta_1 = \beta_2 = 0.1\beta_3 = \eta$, resulting in the additional constraint $J_0^{\eta} = \eta$.

The initial cost function for the reachability calculation is

$$J_0(x,\beta) = \min\{J_0^{\text{radius}}(x), J_0^{\max}(x,\beta), J_0^{\min}(x,\beta), J_0^{\eta}(\beta)\} \tag{20}$$

Figure 7 shows the the resultant reachable set for $\eta = 1.10 \times 10^{-3}$. As opposed to the two previous examples, the safe region lies *outside* of the shaded region. For clarity, the invariant set calculated with dynamics (17) and initial cost function (18) is also displayed in Figure 7, and contains the invariant set calculated with the prescribed controller and initial cost function (20).

4 Recovery from Error

We consider the problem of recovery from error states using formal methods from hybrid control theory. The main objective of this approach is to determine 1) states from which recovery is possible, and 2) controllers to provide guidance during a recovery maneuver from an error state. New methods and tools in hybrid reachability analysis can provide an alternative framework to ad-hoc design for recovery in safety-critical systems with nonlinear continuous dynamics as well as discrete mode-logic. These methods provide a mathematical guarantee of the modeled system's behavior, in the presence of state and input constraints.

We presume real-time failure diagnosis and implementation of control laws for recovery, however simply assessing and correctly identifying failures in real-time is a complicated issue [36, 37, 38]. Recent work in reconfigurable control [39, 40] is based on real-time assessment and control to identify and respond to candidate failures. Other researchers have also explored formal methods for recovery [41, 42, 36, 43] for systems with discrete or simple continuous dynamics, as well as control synthesis for linear systems recovering a tracking trajectory [44].

4.1 Problem Formulation

Consider the nonlinear dynamical system

$$\dot{x} = f(x,u), x \in \mathscr{X} \subseteq \mathbb{R}^n, u \in \mathbb{R} \tag{21}$$

with bounded input $u \in \mathscr{U}^{\text{std}}$, and constraint set $\mathscr{C}^{\text{std}} \subset \mathbb{R}^n$ which encodes the set of states which satisfy the constraints on the system (e.g., speeds above the aircraft's stall speed) during *standard operation*. We express the state constraints through the inequality

$$\mathscr{C}^{\text{std}} = \{x \,|\, c^{\text{std}}(x) \geq 0\}. \tag{22}$$

Define the reachable set as the set of states in $\mathscr{C}^{\text{std}}$ for which all values of a measurable function $u(\cdot)$ in $\mathscr{U}^{\text{std}}$ drive the system state out of the constraint set $\mathscr{C}^{\text{std}}$. We compute the reachable set and its complement, known as the invariant set, through Hamilton-Jacobi techniques.

Statement of Problem 2 *Given the dynamical system (21), with state constraints (22), determine the invariant set $\mathscr{W}^{\text{std}}$, which is the largest set of states x that, despite bounded input $u \in \mathscr{U}^{\text{std}}$, will not violate the state constraints $x \in \mathscr{C}^{\text{std}}$. The invariant set $\mathscr{W}^{\text{std}} \subseteq \mathscr{C}^{\text{std}}$ is the "safe" area of operation.*

The result of the backwards reachability calculation is written as a function of the dynamics in backwards time, the input range, and the constraint set.

$$\begin{array}{rcl} \mathscr{W}^{\text{std}} & = & \text{Reach}(\mathscr{C}^{\text{std}}) \\ \text{subject to } \dot{x} & = & -f(x,u), u \in U^{\text{std}} \end{array} \tag{23}$$

For problems of recovery, we are concerned with states that are outside of the "safe" area but still within a reasonable distance of recovery – these are the error states, or failure states. The size of this region depends on the particular recovery dynamics allowed – significantly larger input bounds, for example, could allow for a much larger recovery region since more control authority can be used to guide the state back to safety. The error state could be the result of a variety of complications, including human error, unanticipated disturbance

or uncontrolled events, faulty sensors, and others. We want to determine, under the temporary *recovery* input and state bounds, which error states can safely reach the safe area of operation, as well as the control law required for recovery to safety. This is a forward reachability problem, since we know the initial states (error states) and want to determine where the state trajectories will evolve to, subject to state constraints.

Statement of Problem 3 *Given the dynamical system (21), with state constraints* $x \in \mathscr{C}^{\text{rcv}} = \{x \,|\, c^{\text{rcv}}(x) \geq 0\}$ *and bounded input* $u \in \mathscr{U}^{\text{rcv}}$*, determine the invariant set* $\mathscr{W}^{\text{rcv}}$ *when starting from the "target" set* $x \in \overline{\mathscr{W}^{\text{std}}}$*, the failure states* $\mathscr{W}^{\text{std}}$ *under standard operation. The solution is trajectories that will reach the target set* $\overline{\mathscr{W}^{\text{std}}}$ *without entering the "avoid" set* $\overline{\mathscr{C}^{\text{rcv}}}$*.*

The result of the forwards reachability calculation is written as a function of the forward-time dynamics, the input range, the target set, and the avoid set.

$$\begin{array}{rcl} \mathscr{W}^{\text{rcv}} & = & \text{ReachAvoid}(\overline{\mathscr{W}^{\text{std}}}, \overline{\mathscr{C}^{\text{rcv}}}) \\ \text{subject to} & & \dot{x} = +f(x,u), u \in \mathscr{U}^{\text{rcv}} \end{array} \tag{24}$$

Note that the result of Problem 2 provides the states from which failure is preventable. Problem 3 presumes failure has occurred, and its result provides 1) the set of failure states for which recovery to standard operation is possible, and 2) the corresponding optimal control law.

4.2 Method

In order to solve Problem 2, we incorporate the state constraints into the initial cost function

$$J_0^{\text{std}}(x) = \max_i c_i^{\text{std}}(x) \tag{25}$$

such that the function is positive in those regions where the constraints are satisfied. We then define the Hamiltonian as

$$H^{\text{std}}\left(x, \frac{\partial J^{\text{std}}}{\partial x}\right) = \max_{u \in \mathscr{U}^{\text{std}}} \left(\frac{\partial J^{\text{std}}}{\partial x}^T f(x,u) \right). \tag{26}$$

The control law which results from (26) will provide envelope protection and despite bounded input. We evolve (25) backwards in time according to (2). The result of this computation is the largest set of states x for a given set of constraints for which trajectories that begin in this set will never violate any state constraints (22) despite bounded input.

In order to solve Problem 3, we incorporate the results of the first reachability calculation. In the forward reachability calculation, we begin with the target, defined as the the failure states resulting from the standard reachability calculation

$$J_0^{\text{rcv}}(x) = -J^{\text{std}}(x) \tag{27}$$

and evolve the cost function forward in time according to the Hamiltonian

$$H^{\text{rcv}}\left(x, \frac{\partial J^{\text{rcv}}}{\partial x}\right) = \max_{u \in \mathscr{U}^{\text{rcv}}} \left(\frac{\partial J^{\text{rcv}}}{\partial x}^T f(x,u) \right), \tag{28}$$

subject to the constraint that states not enter the avoid set. The result is the set of states in the safe envelope that are reachable from failure states – states from which a successfully recovery is possible.

Remark: We have solved the recovery problem through the above two reachability calculations. The first calculation from Problem 2 provides the operating space which must be maintained to prevent entering a failure state. The second calculation from Problem 3 provides information regarding recovery – it identifies those failure states that will lead to recovery as well as the control law which must be applied in order to successfully recover to standard operation. ■

While we have presented our method for the simplest case, a continuous system, this method also generalizes to hybrid systems with both continuous and discrete dynamics. The discrete control can also be calculated through the hybrid reachability algorithm, discussed in detail in [18].

4.3 Examples

Cooperative Collision Avoidance

Consider the collision avoidance scenario with modified turn rates $u_1, u_2 \in \mathscr{U}_{\text{soft}} = 0.75 \cdot \mathscr{U}_{\text{hard}}$, $\mathscr{U}_{\text{hard}} = [-\tan(2\pi/9), \tan(2\pi/9)]$, and constraint set $\mathscr{C}^{\text{std}} = \{x \,|\, J_0^{\text{std}}(x) \geq 0\}$, with modified initial cost function $J_0^{\text{std}}(x) = x_r^2 + y_r^2 - (R+\varepsilon)^2 \geq 0$ where $\varepsilon = 2.5$ nmi provides "padding" against the hard constraints.

Applying the safety/recovery calculation method, we first obtain the safe operating region under the "soft" constraints – this is the set of states from which the aircraft can avoid entering the protective zone. The computed result is the light (yellow) shape shown in the bottom half of Figure 8. However, if for some reason the pilot or the automation does not apply the appropriate control law, an error state will occur. Using hard bounds and constraints, as well as the invariant set from the previous calculation, we can compute the recovery states and controls.

Details of the calculation are included in [45]. The forward reachable (recovery) set $\mathscr{W}^{\text{rcv}}$ is shown in Figure 8. The evolution of the set in forward time is shown in Figure 9 for four values of relative heading θ_r. The sets grow in forward time until they reach the invariant set $\mathscr{W}^{\text{std}}$ under standard operation.

Aborted Automatic Landing

We model the nonlinear longitudinal dynamics of a large civil jet aircraft by $\dot{x} = f_i(x,u)$, in which the state $x = [V, \gamma, h] \in \mathbb{R}^3$ includes the aircraft's speed V, flightpath angle γ, and altitude h (see [46, 18]):

$$\begin{bmatrix} m\dot{V} \\ mV\dot{\gamma} \\ \dot{h} \end{bmatrix} = \begin{bmatrix} -D(\alpha,V) + T\cos\alpha - mg\sin\gamma \\ L(\alpha,V) + T\sin\alpha - mg\cos\gamma \\ V\sin\gamma \end{bmatrix} \tag{29}$$

We assume the control input is $u = [T, \alpha]$, with aircraft thrust T and angle of attack α. The aircraft has mass $m = 190000$ kg, pitch $\theta = \alpha + \gamma$, and gravitational acceleration is $g = 9.81$ m/s^2. The aircraft's lift $L(\alpha,V) = \frac{1}{2}\rho V^2 S C_L(\alpha)$ and drag $D(\alpha,V) = \frac{1}{2}\rho V^2 S C_D(\alpha)$ depend on air density $\rho = 1.225$ kg/m^3, wing surface area $S = 427.80$ m^2, and the coefficients of lift and drag, $C_L(\alpha) = C_{L_0} + C_{L_\alpha}\alpha$ and $C_D(\alpha) = C_{D_0} + K C_L^2(\alpha)$.

The landing aircraft is a hybrid system because the constants C_{L_0}, C_{D_0}, and K vary according to the particular combinations of flap settings and landing gear in an autoland/go-around scenario [46, 47, 48, 49, 50] (Table 1). $C_{L_\alpha} = 5.105$ in all modes. The landing maneuver begins in the Flare-30D, as the aircraft prepares for touchdown on the runway.

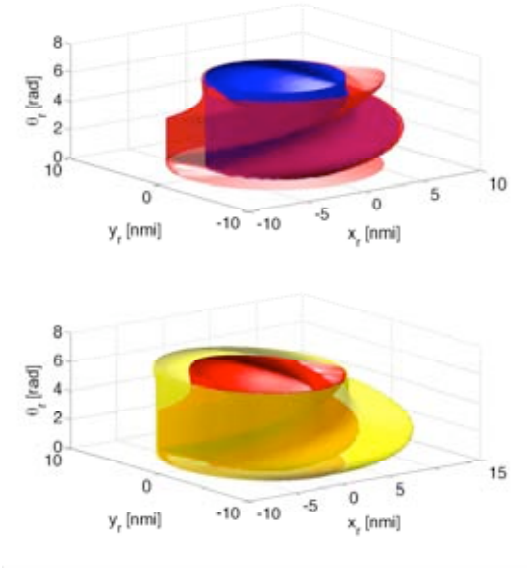

Figure 8: Top figure: The states (x_r, y_r, θ_r) in between the light (red) set $\mathscr{W}^{\text{rcv}}$ and the dark (blue) set $\mathscr{W}^{\text{std}}$ are those failure states from which there exists a control law that will take the system back to the invariant set $\mathscr{W}^{\text{std}}$. The dark (blue) set is the invariant set $\mathscr{W}_{\text{hard}}$, calculated under hard inputs and constraints. Bottom figure: The invariant set $\mathscr{W}^{\text{std}}$ is those states outside of the light (yellow) shape. The recovery set $\mathscr{W}^{\text{rcv}}$ (dark, red) represents those failure states which can reach $\mathscr{W}^{\text{std}}$ (light, yellow).

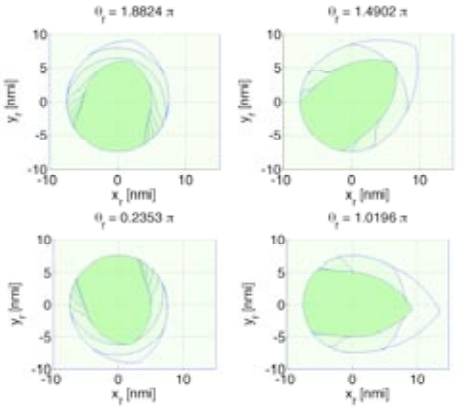

Figure 9: Recovery set in (x_r, y_r) for specific θ_r. The innermost region (shaded) is a cross-section of the reachable set $\mathscr{W}_{\text{hard}}$, the reachable set under hard input and state constraints. The outermost set intersects with the invariant set $\mathscr{W}$, under soft input and state constraints.

If a go-around is required, standard operating procedure calls for a direct series of transitions, Flare-30D $\overset{\text{flaps}}{\rightarrow}$ Go-20D $\overset{\text{gear}}{\rightarrow}$ Go-30D: first the flaps are changed, then the landing gear is retracted. However, as Figure 10 shows, there are significant portions of the aerodynamic flight envelope in Flare-30D from which this maneuver is simply not possible. These states are represented by the mesh-portion of the invariant set $\mathscr{W}_{\text{Flare}-30\text{D}}$, and are outside of the invariant set $\mathscr{W}_{\text{Go}-20\text{U}}$. These states are failure states, since the pilot has no recourse according to this procedure if a go-around is necessary while the aircraft is in the states $x \in \mathscr{W}_{\text{Flare}-30\text{D}} \cap \overline{\mathscr{W}_{\text{Go}-20\text{U}}}$.

We now determine the forward reachable set through a ReachAvoid computation, in order to determine which failure states will, under the recovery input constraints, reach the invariant set $\mathscr{W}_{\text{Go}-30\text{D}}$. For this system, the continuous inputs are already at their limits. However, there is flexibility in the discrete control input – we presume to allow flexibility in choosing the discrete mode. Any go-around mode may be chosen for continuous states that are within its constraint set, as dictated by the (V, γ) limits in Table 1. The computed invariant set is given by

$$\begin{gathered}\mathscr{W}^{\text{rcv}} = \text{ReachAvoid}(W_{\text{Flare}-30\text{D}} \cap \overline{\mathscr{W}_{\text{Go}-20\text{U}}}, \overline{\mathscr{C}^{\text{rcv}}}) \\ \text{s.t. } (29) \text{ for } \{\text{Go-20D, Go-20U, Go-30D, Go-30U}\}\ , u \in \mathscr{U}\end{gathered} \tag{30}$$

The result of the calculation is shown in Figure 11. The original invariant set in Flare, $\mathscr{W}_{\text{Flare}-30\text{D}}$ is fully contained within the forward reachable set, $\mathscr{W}^{\text{rcv}}$. This set was obtained by propagating the failure states

Mode	C_{L_0}	C_{D_0}	K	Flaps	Gear	V [m/s]	γ [degrees]	α [degrees]	T [N]
Flare-30D	0.8212	0.0254	0.04831	F-30	Down	[55.57, 87.46]	$[-6.0°, 0.0°]$	$[-9°, 15°]$	0
Go-20D	0.4225	0.0248	0.04831	F-20	Down	[63.97, 97.74]	$[-6.0°, 13.3°]$	$[-8°, 12°]$	[0, 686700]
Go-30D	0.8212	0.0254	0.04831	F-30	Down	[55.57, 87.46]	$[-6.0°, 15.7°]$	$[-9°, 15°]$	[0, 686700]
Go-20U	0.4225	0.0197	0.04589	F-20	Up	[63.79, 97.74]	$[-6.0°, 13.3°]$	$[-8°, 12°]$	[0, 686700]
Go-30U	0.8212	0.0203	0.04589	F-30	Up	[55.57, 87.46]	$[-6.0°, 15.7°]$	$[-9°, 15°]$	[0, 686700]

Table 1: Aerodynamic constants for autoland modes.

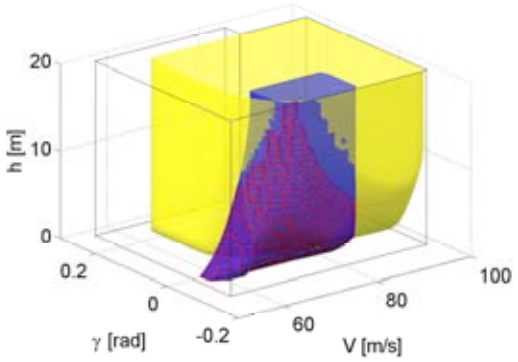

Figure 10: Safe region for landing $\mathscr{W}_{\text{Flare}-30\text{D}}$ (dark, blue) and safe region for go-around (light, yellow) $\mathscr{W}_{\text{Go}-20\text{U}}$. Note the intersection of the two is not fully contained in $\mathscr{W}_{\text{Go}-20\text{U}}$, therefore error states are possible when the pilot attempts to switch from landing to a go-around.

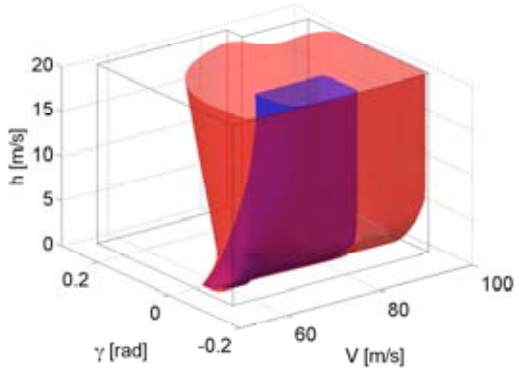

Figure 11: Forward reachable set $\mathscr{W}^{\text{rcv}}$ from Flare-30D mode under recovery dynamics which allow switching between any of four go-around modes, depending on the configuration of the flaps (F-20, F-30) and landing gear (Down, Up).

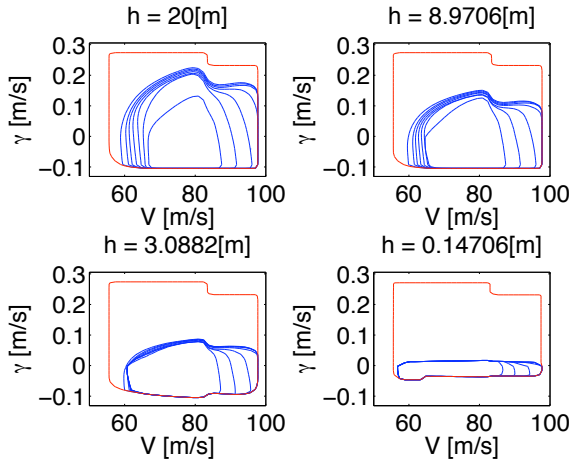

Figure 12: Forward reachable set $\mathscr{W}^{\text{rcv}}$ grows over time (blue). The invariant set for the go-around modes is shown in red, and contains $\mathscr{W}^{\text{rcv}}$. Close to the ground, the reachable set is quite small, since the envelope for landing is narrow compared to the envelopes for go-around. At higher altitudes $\mathscr{W}^{\text{rcv}}$ is considerably larger.

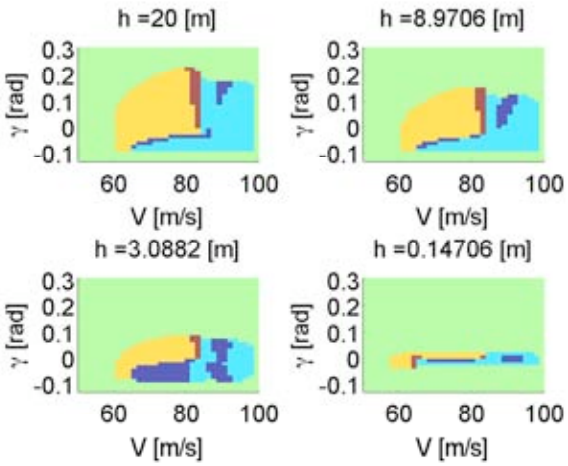

Figure 13: Optimal discrete modes in (V,γ) for various altitudes. The yellow region represents Go-30U, red represents Go-30D, blue represents Go-20U, and cyan represents Go-20D. This control is synthesized during the forward reachability calculation to compute $\mathscr{W}^{\text{rcv}}$.

$\mathscr{W}_{\text{Flare}-30\text{D}} \cap \overline{\mathscr{W}_{\text{Go}-20\text{U}}}$ forward in time while avoiding the exterior of the aerodynamic envelopes for all of the go-around modes.

Cross-sections of the forward-reachable set are shown in Figure 12 at various altitudes. The set is quite restricted near the ground, but grows considerably by the time the aircraft has climbed to 20 m. This reflects the fact that there is a relatively narrow region in (V,γ) for which landing can be accomplished safely. The invariant set $\mathscr{W}^{\text{rcv}}$ grows in forward time, so the outermost set corresponds to surface shown in Figure 11.

This calculation also provides information about the particular continuous and discrete controls that are optimal at every state. Figure 13 shows the optimal modes in the flight envelope (V,γ) at various altitudes. Notice that the inputs correspond to the envelope restrictions imposed during the calculation: the yellow and red areas, representing modes Go-30U and Go-30D, respectively, only occur inside the (V,γ) flight envelopes for those modes. Similarly, the blue and cyan regions, representing modes Go-20U and Go-20D, respectively, occur at higher speeds consistent with the Flaps-20 envelopes.

5 Conclusion

Sections 3 and 4 detailed novel contributions in reachability analysis for human-interaction with complex systems. These contributions were inpsired by real-world problems in aircraft, but are likely to arise in other complex systems, including biomedical devices, driver assistance programs, nuclear surety, the power grid, and other critical infrastructures.

Section 3 presented a method to determine, through a Hamilton-Jacobi reachability computation, the set of states in safety-critical systems which will reach the desired equilibrium without saturating the input or violating the state constraints. Thus both envelope protection and stabilization under saturation are simultaneously achieved. This involves a reachability analysis on an extended state space which incorporates a parameter from the feedback linearizing input. By incorporating the input saturation, stability, and state constraints simultaneously in the initial cost function, the resultant invariant set will be the largest set of states, given bounded input, which will stabilize the system and always remain within a given constraint set.

The work presented contributes to the difficult problem of determining stabilizing controllers for safety-critical systems under nonlinear state and input constraints. Many future directions of work are possible, including 1) minimization of the number of switched, non-saturating controllers when multiple solutions to the control parameterization problem are possible, 2) alternative, less computationally exhaustive formulations to sample the parameter space β and 3) one-step synthesis of a minimal number and optimal selection of input parameters β for switched, non-saturating, feedback linearizing controllers.

Section 4 formulated the recovery problem for hybrid systems with flexibility in continuous inputs, discrete inputs, or state constraints. Standard reachability analysis will reveal those states from which failure is avoidable with the proper choice of control law. In the event that failure does occur, a new forward reachability calculation can identify those failure states from which recovery is possible, as well as the control input (both continuous and discrete) necessary for that recovery. This new calculation exploits the flexibility inherent to the hybrid system – if this flexibility were not present, a recovery calculation would provide no new information from the initial backwards reachability calculation. The recovery calculation involves temporarily adjusting the system's constraints in order to recover to standard operation and standard constraints.

The forward reachability calculation yields not only 1) the forward reachable set from error states, but also 2) the control law required to achieve that set. These two case studies provide interesting motivation for further work in synthesizing recovery maneuvers. Future work will proceed in comparing the forward reachability result with a converse problem in which the standard operating region is propagated backwards in time under the new recovery dynamics.

Two real-world examples were presented to illustrate both methods: 1) longitudinal aircraft dynamics, and two-aircraft lateral collision avoidance dynamics. The dynamics for both examples are derived from physical models of civil jet aircraft.

References

[1] J. Rushby. Modeling the human in human factors (extended abstract). In Udo Voges, editor, SAFECOMP *2001: Proceedings of the 20th International Conference on Computer Safety, Reliability, and Security*, volume 2187 of *Lecture Notes in Computer Science*, pages 86–91, Budapest, Hungary, September 2001. Springer-Verlag.

[2] S. Vakil, A. Midkiff, T. Vaneck, and R. Hansman. Mode awareness in advanced autoflight systems. In *Proceedings of the 6th IFAC/IFIP/IFORS/IEA Symposium on Analysis, Design, and Evaluation of Man-Machine Systems*, Cambridge, MA, 1995.

[3] J. Crow, D. Javaux, and J. Rushby. Models and mechanized methods that integrate human factors into automation design. In *International Conference on Human-Computer Interaction in Aeronautics*, Toulouse, France, September 2000.

[4] M. Amin. Security challenges for the electricity infrastructure. *Computer*, 35(4):8–10, April 2002.

[5] C. Billings. *Aviation Automation: The Search for a Human-Centered Approach*. Erlbaum, Hillsdale, NJ, 1997.

[6] K. Abbott, S. Slotte, and D. Stimson. The interfaces between flightcrews and modern flight deck systems. Human Factors Team Report, Federal Aviation Administration, June 1996.

[7] P. Beerthuizen. Designing for failure. In *European Space Agency Special Publication*, pages 667–670, Prague, Czech Republic, 2003.

[8] E. Palmer. Oops, it didn't arm - a case study of two automation surprises. In *8th International Symposium on Aviation Psychology*, Columbus, Ohio, 1995.

[9] C. Tomlin, J. Lygeros, and S. Sastry. A game theoretic approach to controller design for hybrid systems. *Proceedings of the IEEE*, 88(7):949–970, 2000.

[10] M. Oishi, I. Mitchell, A. Bayen, C. Tomlin, and A. Degani. Hybrid verification of an interface for an automatic landing. In *Proceedings of the IEEE Conference on Decision and Control*, pages 1607–1613, Las Vegas, NV, December 2002.

[11] I. Mitchell, A. M. Bayen, and C. J. Tomlin. A time-dependent Hamilton-Jacobi formulation of reachable sets for continuous dynamic games. *IEEE Transactions on Automatic Control*, 50(7):947–957, July 2005.

[12] Ian Mitchell. *A Toolbox of Level Set Methods*. Department of Computer Science, University of British Columbia, June 2004. www.cs.ubc.ca/ mitchell/ToolboxLS.

[13] J.-P. Aubin. *Viability Theory*. Birkhauser, 1991.

[14] P. Saint-Pierre. Approximation of the viability kernel. *Applied Mathematics and Optimisation*, 29:187–209, 1994.

[15] J.-P. Aubin, J. Lygeros, M. Quincampoix, S. Sastry, and N. Seube. Impulse differential inclusions: a viability approach to hybrid systems. *IEEE Transactions on Automatic Control*, 47(1):2–20, 2002.

[16] P. Saint-Pierre. Approximation of viability kernels and capture basin for hybrid systems. In J.L. Martins de Carvalho, editor, *European Control Conference*, pages 2776–2783, 2001.

[17] E. Cruck and P. Saint-Pierre. Nonlinear impulse target problems under state constraint: A numerican analysis based on viability theory. *Set-Valued Analysis*, 12(4):383–416, December 2004.

[18] C. Tomlin, I. Mitchell, A. Bayen, and M. Oishi. Computational techniques for the verification of hybrid systems. *Proceedings of the IEEE*, 91(7):986–1001, 2003.

[19] M. Fliess, J. Levin, P. Martin, and P. Rouchon. A Lie-Backlund approch to equivalence and flatness of nonlinear systems. *IEEE Transactions on Automatic Control*, 44(5):922–937, 1999.

[20] R. Hirschorn and J. Davis. Global output tracking for nonlinear systems. *SIAM Journal of Control and Optimization*, 26(6):1321–1330, 1988.

[21] A. Bemporad. Reference governor for constrained nonlinear systems. *IEEE Transactions on Automatic Control*, 43(3):415–419, 1998.

[22] G. Pappas, J. Lygeros, and D. Godbole. Stabilization and tracking of feedback linearizable systems under input constraints. In *Proceedings of the IEEE Conference on Decision and Control*, pages 596–601, New Orleans, LA, December 1995.

[23] N. Kapoor and P. Daoutidis. Stabilization of unstable systems with input constraints. In *Proceedings of the American Control Conference*, pages 3192–3196, Seattle, WA, June 1995.

[24] F. Doyle. An anti-windup input-output linearization scheme for SISO systems. *Journal of Process Control*, 9:213–220, 1999.

[25] P. Lu. Tracking control of nonlinear systems with bounded controls and control rates. *Automatica*, 33(6):1199–1202, 1997.

[26] N. Faiz, S. Agrawal, and R. Murray. Differentially flat systems with inequality constraints: An approach to real-time feasible trajectory generation. *Journal of Guidance, Control, and Dynamics*, 24(2):219–227, 2001.

[27] P. Martin, R. Murray, and P. Rouchon. Flat systems, equivalence, and trajectory generation. Technical report, Caltech Technical Report, California Institute of Technology, Pasadena, CA, 2003.

[28] W. Liao, M. Cannon, and B. Kouvaritakis. Constrained MPC using feedback linearization for systems with unstable inverse dynamics. In *Proceedings of the American Control Conference*, pages 846–851, Portland, OR, June 2005.

[29] M. Bacic, M. Cannon, and B. Kouvaritakis. Invariant sets for feedback linearisation based on nonlinear predictive control. *IEE Proceedings in Control Theory Applications*, 152(3):259–265, 2005.

[30] V. Nevistic and J. Primbs. Model predictive control: Breaking through constraints. In *Proceedings of the IEEE Conference on Decision and Control*, pages 3932–3937, December 1996.

[31] N. El-Farra and P. Cristofides. Switching and feedback laws for control of constrained switched nonlinear systems. In C. Tomlin and M. Greenstreet, editors, *Hybrid Systems: Computation and Control*, LNCS 2289, pages 164–178. Springer-Verlag, March 2002.

[32] Y. Lin and E. Sontag. A universal formula for stabilization with bounded controls. *Systems and Control Letters*, 16:393–397, 1991.

[33] M. S. Branicky. Multiple Lyapunov functions and other tools for switched and hybrid systems. *IEEE Transactions on Automatic Control*, 43(4):475–482, 1998.

[34] T. Hu and Z. Lin. Composite quadratic lyapunov functions for constrained control systems. *IEEE Transactions on Automatic Control*, 48(3):440–450, 2003.

[35] I. Mitchell and C. Tomlin. Level set methods for computation in hybrid systems. In B. Krogh and N. Lynch, editors, *Hybrid Systems: Computation and Control*, LNCS 1790. Springer Verlag, March 2000.

[36] J. Rushby. Formal specification and verification of a fault-masking and transient-recovery model for digital flight-control systems. Technical report, NASA Contrator Report N-4384, NASA Ames Research Center, Moffett Field, CA, July 1991.

[37] J. Boskovic, S. Bergstrom, and R. Mehra. Retrofit reconfigurable flight control in the presence of control effector damage. In *Proceedings of the American Control Conference*, pages 2652–2657, Portland, OR, 2005.

[38] H. Zhang, W.S. Gray, and O. Gonzalez. Performance analysis of recoverable flight control systems using hybrid dynamical models. In *Proceedings of the American Control Conference*, pages 2787–2792, Portland, OR, 2005.

[39] S. Glavaski, M. Elgersma, M. Dorneich, and P. Lommel. Failure accommodating aircraft control. In *Proceedings of the American Control Conference*, pages 3624–3630, Anchorage, AK, 2002.

[40] M. Elgerma and S. Glavaski. Reconfigurable control for active management of aircraft system failures. In *Proceedings of the American Control Conference*, pages 2627–2639, Arlington, VA, 2001.

[41] R. Butler, J. Maddalon, A. Geser, and C. Munoz. Formal analysis of air traffic management systems: the case of conflict resolution and recovery. In *Proceedings of the Winter Simulation Conference: Driving Innovation*, volume 1, pages 906–914, New Orleans, LA, 2003.

[42] M. Akatsu, T. Murata, and K. Kurihara. Verification of error recovery specification for distributed data by using colored petri net. In *Proceedings of the IEEE Interantional Symposium on Circuits and Systems*, volume 2, pages 930–933, Singapore, 1991.

[43] P. Naldurg and R. Campbell. Modeling insecurity: Policy engineering for survivability. In *Proceedings of the ACM Workshop on Survivable and Self-Regenerative Systems*, pages 91–98, 2003.

[44] S. Devasia and G. Meyer. Recovery guidance for linear systems with input and state constraints. In *Proceedings of the American Control Conference*, pages 1122–1127, Philadelphia, PA, 1998.

[45] M. Oishi. Recovery from error in flight management systems: Applications of hybrid reachability. In *IEEE Advanced Process Controls Workshop*, Vancouver, BC, 2006.

[46] A. Bayen and C. Tomlin. Nonlinear hybrid automaton model for aircraft landing. SUDAAR 737, Dept. of Aeronautics and Astronautics, Stanford University, Stanford, CA, 2001.

[47] S. Rogers, K. Roth, H. Cao, J. Slotnick, M. Whitlock, S. Nash, and M. Baker. Computation of viscous flow for a Boeing 777 aircraft in landing configuration. In *AIAA Conference Proceedings*, number 2000-4221, October 1992.

[48] J. Roskam and C.-T. Lan. *Airplane Aerodynamics and Performance*. Design, Analysis, and Research Corporation, Lawrence, Kansas, 1997.

[49] A. Flaig and R. Hilbig. High-lift design for large civil aircraft. In *AGARD Conference Proceedings 515*, France, October 1992.

[50] L. Jenkinson, P. Simpkin, and D. Rhodes. *Civil Jet Aircraft Design*. American Institute of Aeronautics and Astronautics, Inc., Reston, VA, 1999. http://www.bh.com/companions/aerodata.

DISTRIBUTION:

1 MS 0123
Yolanda Moreno, 1010

1 MS 0123
Marie L. Garcia, 1010

1 MS 0123
Henry R. Westrich, 1011

1 MS 0511
Wendy R. Cieslak, 1010

1 MS 0513
Richard R. Stulen, 1000

1 MS 1138
Steve Kleban, 6226

1 MS 1138
Robert J. Glass, 6226

2 MS 9018
Central Technical Files, 8945-1

2 MS 0899
Technical Library, 4536